

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

15 - 0566 JMC

IN THE MATTER OF THE SEARCH)
OF THE PREMISES KNOWN AS:) CASE NO.
640 N. CALVERT STREET, APT D)
BALTIMORE, MARYLAND 21202)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Todd A. Moody, a Baltimore City Police Detective/Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), Baltimore Division, Baltimore, Maryland, being duly sworn, depose and state as follows:

1. I have been a Police Officer since 1997, and a Detective/Task Force Officer (TFO) with the FBI since 1999. I currently investigate state and federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have obtained FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer-to-Peer Network Online Investigation training. I have also participated in the execution of numerous search warrants, many of which have involved child exploitation and/or child pornography offenses.

2. As a TFO, I am authorized to investigate violations of laws of the United States and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a search warrant to search the premises located at 640 N. Calvert Street, Apt D, Baltimore, Maryland 21202 ("SUBJECT PREMISES"), more particularly described in Attachment A, for evidence of violations of Title

JTM
2013/20230

18, United States Code, Section 2252A(a)(1) and (2) (transportation and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography). The purpose of this application is to seize and search evidence, more particularly described in Attachment B, as evidence, fruits, and instrumentalities of criminal activity.

4. The statements in this affidavit are based in part on information provided by Special Agents of the FBI and/or Task Force Officers, and employees of the Department of Justice's Child Exploitation and Obscenity Section ("CEOS"), and on my experience and background as a Task Force Officer with the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that Your Affiant believes are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Section 2252A(a)(1) and (2) (transportation and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B)(possession of child pornography), are presently located at the SUBJECT PREMISES.

5. For the reasons set forth below, there is probable cause to believe that the SUBJECT PREMISES contain evidence of violations of Title 18, United States Code, Section 2252A.

PEER-TO-PEER FILE SHARING

6. Peer-to-peer file sharing (hereinafter "P2P") is a method of communication available to Internet users through the use of special software that allows users to trade digital files through P2P networks formed by linking computers together through the Internet. A user first obtains the P2P software, which can be downloaded from the internet. In general, P2P

software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Some types of P2P software set up their searches by keyword. The results of the keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

7. For example, a person interested in obtaining visual depictions of minors engaged in sexually explicit conduct would open the P2P application on his/her computer and, using a term such as "preteen sex," conduct a search of a P2P network for computers sharing files associated with that term. The user can then select files from the search results and download them directly from the computer(s) sharing those files. The download of a file occurs through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored on the requesting user's computer in the area previously designated by the requesting user and will remain there until moved or deleted.⁴

8. One of the advantages of P2P file sharing is that a user can download multiple files in parallel. This means that a user can download more than one file at a time. In addition, a user can download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it reduces the time it takes to download a file.

9. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible

for data to be transferred between computers.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

10. Searches and seizures of evidence from computers and internet accessible mobile devices commonly require agents to download or copy information from the devices and their components, or seize most or all device-related items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like smart phones, gaming consoles, Blu-ray players, hard drives, USB or thumb drives, DVDs, CDs, tapes, laser disks, and other digital storage devices) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching computer systems and digital devices for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal

activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

11. To fully retrieve data from a computer system, the analyst needs all storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

**SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO
POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF
COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT
AND DISTRIBUTION OF CHILD PORNOGRAPHY**

12. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet generally, and Peer to Peer applications specifically, to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names,

addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge on how to access a Peer to Peer network to distribute and possess child pornography to others would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

13. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

a. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they

are overwritten.

b. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

c. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

d. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above described information will be recovered during forensic analysis.

14. Based on traits shared by collectors, the ability of a forensic analyst to find data long after it has been deleted, and the increased storage capacity of computers over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found at the target residence notwithstanding the passage of time. In addition, based on this target's activity, detailed below, which consisted of making at least three image files available for others to download via a peer-to-peer network depicting child pornography, there is reason to believe the target has both collected images of child pornography and distributed child pornography.

SUMMARY OF INVESTIGATION

15. On or about December 28, 2014, a Special Agent with the FBI, herein referred to as OCE-6178, located in Newark, New Jersey, and acting in an undercover capacity, used a Peer-to-Peer (P2P) file sharing program, hereafter referred to as the P2P client. OCE-6178 logged onto the P2P client network and observed an individual utilizing the user name, "Jtmdterps1", was logged into the network. "Jtmdterps1" was sharing 3 read only folders titled, "jtmdterps1", "New Folder", and New Folder 2".

16. OCE-6178 browsed Jtmdterps1's shared folders. OCE-6178 previewed the image files "Jtmdterps1" was sharing in thumbnail view and observed images depicting child pornography and video files with titles indicative of child pornography. "Jtmdterps1" was sharing 196 files.

17. On December 28, 2014, between 9:30 AM and 10:15 AM, Eastern Standard Time (EST), OCE-6178 successfully completed a download of 80 files from a computer whose user was connected via IP address "68.48.158.62". Those files were copied to a disc and forwarded to your affiant with an investigative lead.

18. I conducted a review of a disc containing a copy of 80 files downloaded by OCE-6178 from the computer using IP address "68.48.158.62" and found files that contained depictions of child pornography. The following are examples of some of these downloaded files:

- a. "- 10yrolsckcock.jpg" - an image file of a prepubescent boy. An adult male is inserting his penis into the child's mouth.
- b. "6af6.jpg" - an image file depicting a prepubescent boy with his genitals exposed with his penis inserted into the mouth of a second prepubescent boy.

- c. "5485247xEx.jpg" – an image file depicting a nude prepubescent boy with his legs spread. A black dildo is inserted and penetrating the boys anus.

19. I reviewed the images/video files obtained from a computer utilizing IP address "68.48.158.62", and concluded, based on my training and experience, that the images are child pornography.

20. Using publicly available websites, OCE-6178 determined that IP Address "68.48.158.62" was an IP address controlled by the Internet Service Provider (ISP) Comcast Cable Communications Inc.

21. OCE-6178 sent a subpoena for the Comcast Cable Communications Inc electronic customer data associated with IP address "68.48.158.62", which is the IP address OCE-6178 obtained the downloads of the aforementioned images from on December 18, 2014 from 9:30 AM and 10:15 AM (EST).

22. Comcast Cable Communications Inc responded to the subpoena and identified the subscriber as follows:

Name: Mr Greg Stocks

Address: 640 N. Calvert Street, Apt. D, Baltimore, Maryland 21202

Phone: 410-913-4337

Email User IDs: gregsto@comcast.net, jtodd88@comcast.net

23. A browse of the Maryland Motor Vehicle Administration database for Gregory Stocks resulted in the following:


Name: Gregory Gerard Stocks, 6'2, 215 lbs, DOB XX-XX-1964

Address: 640 N. Calvert Street, Apt D, Baltimore, Maryland 21202

CONCLUSION

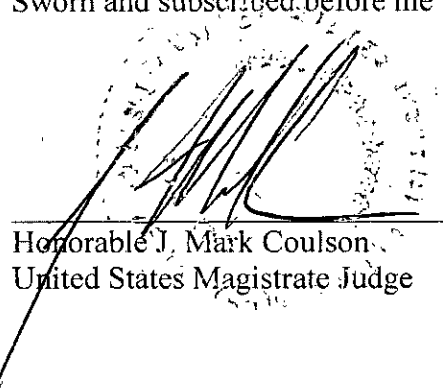
24. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A are located at the SUBJECT PREMISES described in Attachment A.

25. In consideration of the foregoing, I respectfully request that this Court issue a warrant to search the SUBJECT PREMISES, as more particularly described in Attachment A, and to seize the items specified in Attachment B.

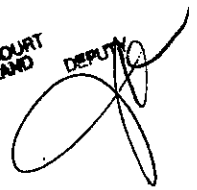


TFO/Detective Todd A. Moody
Federal Bureau of Investigation
Baltimore City Police Department

Sworn and subscribed before me this 24 day of March 2015



Honorable J. Mark Coulson
United States Magistrate Judge

FILED ENTERED
LOGGED RECEIVED
APR 07 2015
AT BALTIMORE
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY 

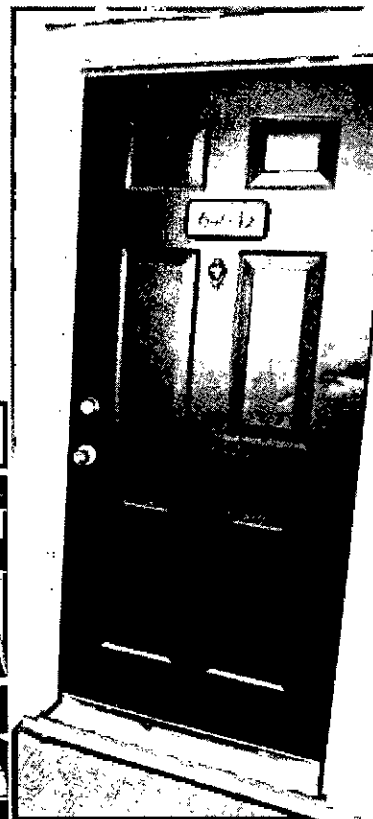
15 - 0566 JMC

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The location known as 640 N. Calvert Street, Apartment D, Baltimore, Maryland 21202 a four story red brick and concrete apartment complex with secured entrances and underground parking.

The front of the home is approachable via the street facing balcony once reaching the fourth level. The front inward opening door is black. The numbers "640D" are in black, affixed to a brass plaque that is attached to the entry door.



FILED _____ ENTERED _____
LODGED _____ RECEIVED _____

APR 07 2015

AT BALTIMORE
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND

BY

DEPUTY

A handwritten signature in black ink, likely belonging to the Deputy Clerk mentioned in the stamp.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), computer hardware, software, related documentation, passwords, data security devices, videotapes, video recording devices, video recording players, monitors, and or televisions, flatbed scanners, electronic devices capable of connecting to the internet or storing electronic data such as tablets, PDAs, and similar electronic devices and data that may constitute instrumentalities of, or contain evidence related to, the crimes set for in the accompanying Affidavit.
2. Any and all web cameras, cameras, film, cell phones with cameras and/or Internet capability, or other photographic equipment.
3. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, Section 2256(8).
4. Any and all correspondence identifying persons transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
5. Any and all records, documents, invoices and materials that concern any accounts with any Internet Service Provider.
6. Any and all visual depictions of minors.
7. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States Mails or by computer, and visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
8. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
9. Any and all documents, records, or correspondence pertaining to occupancy at 640 N. Calvert Street, Apt. D, Baltimore Maryland 21202.
10. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
11. Any and all records relating to persuading, inducing, enticing or coercing any minor to engage in any sexual activity in violation of the law.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

12. For any computer, computer hard drive, or other physical object upon which computer data can be recorded including but not limited to tablets, PDAs, and other electronic devices (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment.

13. Any of the items described in paragraphs 1 through 12 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form. The search procedure of the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the

search will view information not within the scope of the warrant:

- a. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
 - b. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
 - c. “scanning” storage areas to discover and possibly recover recently deleted files;
 - d. “scanning” storage areas for deliberately hidden files; or
 - e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.
14. If after performing these procedures, the directories, files or storage areas do not reveal evidence of fraud or financial crimes and items that related to or constitute evidence, fruits, or instrumentalities of violations of for evidence of violations of Title 18, United States Code, Section 2252A(a)(1) and (2) (transportation and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography), et seq., the further search of that particular directory, file or storage area, shall cease.

FILED _____ ENTERED _____
LODGED _____ RECEIVED _____
APR 07 2015
AT BALTIMORE
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ DEPUTY

